


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: The ACM Digital Library The Guide

Nothing Found

Your search for **without <near/6> browser <and> send* <near/6> unencrypt* <near/3> URL** did not return any results.

with date search

You may want to try an [Advanced Search](#) for additional options.

Please review the [Quick Tips](#) below or for more information see the [Search Tips](#).

Quick Tips

- Enter your search terms in lower case with a space between the terms.

`sales offices`

You can also enter a full question or concept in plain language.

`Where are the sales offices?`

- Capitalize proper nouns to search for specific people, places, or products.

`John Colter, Netscape Navigator`

- Enclose a phrase in double quotes to search for that exact phrase.

`"museum of natural history" "museum of modern art"`

- Narrow your searches by using a **+** if a search term must appear on a page.

`museum +art`

- Exclude pages by using a **-** if a search term must not appear on a page.

`museum -Paris`

Combine these techniques to create a specific search query. The better your description of the information you want, the more relevant your results will be.

`museum +"natural history" dinosaur -Chicago`

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)



[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: The ACM Digital Library The Guide

without <near/6> browser <and> send* <near/6> unencrypt*

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used

[without near/6 browser](#) and [send near/6 unencrypt](#) [near/3 URL](#)

Found 17,248 of 166,953

Sort results by

relevance

[Save results to a Binder](#)

Try an [Advanced Search](#)

Display results

expanded form

[Search Tips](#)
 [Open results in a new window](#)

Try this search in [The ACM Guide](#)

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

- 1 [Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks](#)

Haidong Xia, José Carlos Brustoloni

May 2005 **Proceedings of the 14th international conference on World Wide Web**
WWW '05

Publisher: ACM Press

Full text available: [pdf\(770.11 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

Keywords: HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

- 2 [Nark: receiver-based multicast non-repudiation and key management](#)

Bob Briscoe, Ian Fairman

November 1999 **Proceedings of the 1st ACM conference on Electronic commerce**

Publisher: ACM Press

Full text available: [pdf\(168.86 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: Internet, audit trail, key management, multicast, non-repudiation, smartcard, watermark

- 3 [The battle against phishing: Dynamic Security Skins](#)

Rachna Dhamija, J. D. Tygar

July 2005 **Proceedings of the 2005 symposium on Usable privacy and security**
SOUPS '05

Publisher: ACM Press

Full text available: [pdf\(398.10 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Phishing is a model problem for illustrating usability concerns of privacy and security because both system designers and attackers battle using user interfaces to guide (or

misguide) users. We propose a new scheme, Dynamic Security Skins, that allows a remote web server to prove its identity in a way that is easy for a human user to verify and hard for an attacker to spoof. We describe the design of an extension to the Mozilla Firefox browser that implements this scheme. We present two novel inte ...

4 Applications: YouServ: a web-hosting and content sharing tool for the masses

◆ Roberto J. Bayardo Jr., Rakesh Agrawal, Daniel Gruhl, Amit Somani
May 2002 Proceedings of the 11th international conference on World Wide Web

Publisher: ACM Press

Full text available:  pdf(238.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

YouServ is a system that allows its users to pool existing desktop computing resources for *high availability* web hosting and file sharing. By exploiting standard web and internet protocols (e.g. HTTP and DNS), YouServ does not require those who access YouServ-published content to install special purpose software. Because it requires minimal server-side resources and administration, YouServ can be provided at a very low cost. We describe the design, implementation, and a successful intrane ...

Keywords: decentralized systems, p2p, peer-to-peer networks, web hosting

5 Protecting Your Site with Access Controls

Reuven M. Lerner
May 1998 Linux Journal

Publisher: Specialized Systems Consultants, Inc.

Full text available:  html(26.16 KB) Additional Information: [full citation](#), [references](#), [index terms](#)

6 Columns: Risks to the public in computers and related systems

◆ Peter G. Neumann
January 2001 ACM SIGSOFT Software Engineering Notes, Volume 26 Issue 1

Publisher: ACM Press

Full text available:  pdf(3.24 MB) Additional Information: [full citation](#)

7 Posters: Exploiting the web for point-in-time file sharing

◆ Roberto J. Bayardo, Sebastian Thomschke
May 2005 Special interest tracks and posters of the 14th international conference on World Wide Web

Publisher: ACM Press

Full text available:  pdf(246.81 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We describe a simple approach to "point-in-time" file sharing based on time expiring web links and personal web servers. This approach to file sharing is useful in environments where instant messaging clients are varied and don't necessarily support (compatible) file transfer protocols. We discuss the features of such an approach along with a successfully deployed implementation now in wide use throughout the IBM corporation.

Keywords: file sharing, instant messaging, personal web server

8 DOS protection: Using graphic turing tests to counter automated DDoS attacks

◆ **against web servers**
 William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, Dan Rubenstein

October 2003 Proceedings of the 10th ACM conference on Computer and communications security

Publisher: ACM PressFull text available:  pdf(256.83 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present WebSOS, a novel overlay-based architecture that provides guaranteed access to a web server that is targeted by a denial of service (DoS) attack. Our approach exploits two key characteristics of the web environment: its design around a human-centric interface, and the extensibility inherent in many browsers through downloadable "applets." We guarantee access to a web server for a large number of *previously unknown* users, without requiring pre-existing trust relationships between ...

Keywords: Java, graphic turing tests, web proxies**9 The Jupiter audio/video architecture: secure multimedia in network places** 

 Pavel Curtis, Michael Dixon, Ron Frederick, David A. Nichols
January 1995 **Proceedings of the third ACM international conference on Multimedia**

Publisher: ACM PressFull text available:  htm(72.37 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**Keywords:** audio, collaboration, encryption, multicast, network places, security, video**10 Access control with IBM Tivoli access manager** 

 Günter Karjoh
May 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 2

Publisher: ACM PressFull text available:  pdf(367.07 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Web presence has become a key consideration for the majority of companies and other organizations. Besides being an essential information delivery tool, the Web is increasingly being regarded as an extension of the organization itself, directly integrated with its operating processes. As this transformation takes place, security grows in importance. IBM Tivoli Access Manager offers a shared infrastructure for authentication and access management, technologies that have begun to emerge in the com ...

Keywords: Access control, WWW security, Web servers, authorization management**11 Risks to the public: Risks to the public** 

 Peter G. Neumann
May 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 3

Publisher: ACM PressFull text available:  pdf(177.87 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, hardware, people, and other circumstances relating to computer systems. To economize on space, we include pointers to items in the online Risks Forum: (R i j) denotes RISKS vol i number ...

12 Columns: Risks to the public in computers and related systems 

 Peter G. Neumann
March 2002 **ACM SIGSOFT Software Engineering Notes**, Volume 27 Issue 2

Publisher: ACM Press

Full text available: Additional Information:

[pdf\(1.54 MB\)](#)[full citation](#)**13 Client-side caching for TLS**

 Hovav Shacham, Dan Boneh, Eric Rescorla
November 2004 **ACM Transactions on Information and System Security (TISSEC)**,
Volume 7 Issue 4

Publisher: ACM PressFull text available: [pdf\(182.01 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We propose two new mechanisms for caching handshake information on TLS clients. The "fast-track" mechanism provides a client-side cache of a server's public parameters and negotiated parameters in the course of an initial, enabling handshake. These parameters need not be resent on subsequent handshakes. Fast-track reduces both network traffic and the number of round trips, and requires no additional server state. These savings are most useful in high-latency environments such as wireless network ...

Keywords: Bloom filters, TLS, session cache, wireless networks**14 Article abstracts with full text online: Risks to the public in computers and related systems**

 Peter G. Neumann
January 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 1

Publisher: ACM PressFull text available: [pdf\(211.64 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, hardware, people, and other circumstances that affect computer systems. To economize on space, we tersify most items and include pointers to items in the online Risks Forum: (R i j) deno ...

15 Risks to the public: Risks to the public in computers and related systems

 Peter G. Neumann
January 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 1

Publisher: ACM PressFull text available: [pdf\(211.64 KB\)](#) Additional Information: [full citation](#), [index terms](#)**16 Inside risks: How secure is secure Web browsing?**

 Albert Levi
July 2003 **Communications of the ACM**, Volume 46 Issue 7

Publisher: ACM PressFull text available: [pdf\(39.66 KB\)](#) Additional Information: [full citation](#), [index terms](#)
[html\(7.55 KB\)](#)**17 Privacy in browser-based attribute exchange**

 Birgit Pfitzmann, Michael Waidner
November 2002 **Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society**

Publisher: ACM PressFull text available: [pdf\(168.95 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Browser-based attribute-exchange protocols enable users of normal web browsers to conveniently send attributes, such as authentication or demographic data, to web sites.

Such protocols might become very common and almost mandatory in general consumer scenarios over the next few years. We derive the privacy requirements on such protocols from general privacy principles and study their consequences for the protocol design. We also survey to what extent proposals like Microsoft's Passport, IBM's e- ...

Keywords: BBAE, Liberty, Passport, SAML, Shibboleth, attribute-exchange, e-Community Single Signon, identity management, privacy, roles, security, single signon, traffic data, wallet, web browser

18 Risks to the public in computers and related systems



Peter G. Neumann

January 2002 **ACM SIGSOFT Software Engineering Notes**, Volume 27 Issue 1

Publisher: ACM Press

Full text available: [pdf\(1.41 MB\)](#) Additional Information: [full citation](#)

19 HTTP Cookies: Standards, privacy, and politics



David M. Kristol

November 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 2

Publisher: ACM Press

Full text available: [pdf\(390.38 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

How did we get from a world where cookies were something you ate and where "nontechies" were unaware of "Netscape cookies" to a world where cookies are a hot-button privacy issue for many computer users? This article describes how HTTP "cookies" work and how Netscape's original specification evolved into an IETF Proposed Standard. I also offer a personal perspective on how what began as a straightforward technical specification turned into a political flashpoint when it tried to address nontechn ...

Keywords: Cookies, HTTP, World Wide Web, privacy, state management

20 The architecture of robust publishing systems



Marc Waldman, Aviel D. Rubin, Lorrie Faith Cranor

November 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 2

Publisher: ACM Press

Full text available: [pdf\(680.21 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Internet in its present form does not protect content from censorship. It is straightforward to trace any document back to a specific Web server, and usually directly to an individual. As we discuss below, there are valid reasons for publishing a document in a censorship-resistant manner. Unfortunately, few tools exist that facilitate this form of publishing. We describe the architecture of robust systems for publishing content on the Web. The discussion is in the context of Publius, as that ...

Keywords: Censorship resistance, Web publishing

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3840	URL near6 transmit\$6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:40
L2	0	L1 near7 without near6 encrypt\$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:41
L3	0	L1 near7 "without" near6 encrypt\$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:41
L4	29	unencrypt\$3 near6 URL	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:55
L5	3597	709/217.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:55
L6	3370	709/219.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:55
L7	2609	709/229.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:58
L8	95	(L5 or L6 or L7) and Internet-enabled	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:58

L9	4	(L5 or L6 or L7) and Internet-enabled near10 without	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/22 09:59
----	---	--	---	----	----	------------------